Adobe LiveCycle Data Services Using the F5 BIG-IP LTM

APPLIES TO

Adobe® LiveCycle® Enterprise Suite

CONTENTS

Introduction

This document contains essential channel configurations and a configuration that is used for near real-time messaging testing. This configuration was optimized for low message latency in our lab. The devices that were used are listed below. All devices were in different subnets in a 1 gigabit network.

- LiveCycle Data Services server: HP ProLiant DL38O
- LiveCycle Data Services edge server: HP ProLiant DL38O G6
- BIG-IP Local Traffic Manager (LTM): F5 3600

This document describes how to connect and use LiveCycle Data Services, LiveCycle Data Services edge server, and BIG-IP LTM together. In this configuration, the BIG-IP LTM machine performs the following tasks:

- Load balancing
- SSL termination (thereby optionally offloading the SSL decryption for Real Time Messaging Protocol over SSL (RTMPS) or HTTPS to the F5 BIG-IP machine)
- HTTP-based authentication

BIG-IP LTM is capable of handling traffic volumes from 1-12 gigabits per second, depending on which model is used.

LiveCycle Data Services edge server can pre-authenticate connections before it proxies connections back to a LiveCycle Data Services instance. If authentication is enabled between the edge and server tiers, anonymous connections are prohibited. If authentication is disabled between the edge and server tiers, there is effectively no functional difference between an F5 BIG-IP LTM to edge tier to server tier configuration, compared to an F5 BIG-IP LTM to server tier (for example, no edge tier) configuration.

If there is a large amount of immutable data that is being fetched and used in the application, cache it when accessing it for the first time. For further use access the data from the cache to improve server's performance.

Adobe

Edge server architecture

The LiveCycle Data Services edge server is placed in the DMZ to route authenticated or authorized connections to the Data Services server. With SSL termination, the F5 BIG-IP LTM system is placed in front of the Data Services edge server.

Architecture overview

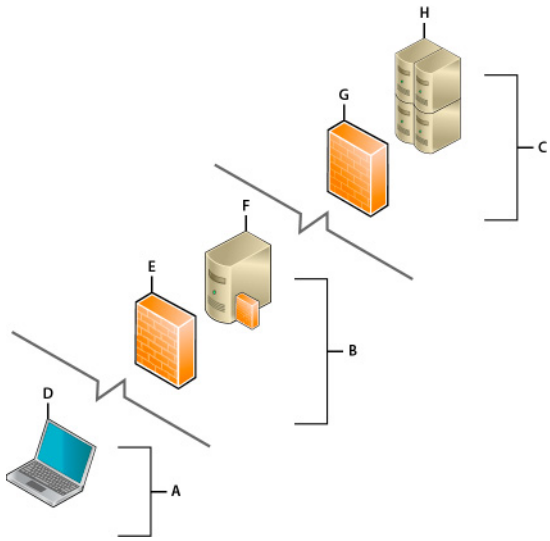
In an enterprise network topology, clients connect to a LiveCycle Data Services edge server or to the F5 BIG-IP LTM. The channel classes must match their protocol. The ActionScript clients use the class defined in the channel definition. The LiveCycle Data Services server uses the endpoint class.

If SSL termination is configured on the F5 BIG-IP, the channel class is a secure channel, and the endpoint is not. Adobe® Flash® Player security does not allow an application to connect to any location other than the place where the application is loaded. You must use a crossdomain.xml file that is specified either in a channel definition or NIO server to get client load balancing or failover to work.

Using the BIG-IP LTM for SSL termination not only offloads processing to the BIG-IP LTM away from the server, but also aids troubleshooting because traffic is decrypted and does not require you to catch the three-way handshake and operations that are processing the certificate's key to decrypt the traffic.

Note: For information about BIG-IP LTM functions, see its documentation.

It is recommended to use a BIG-IP health monitor when you configure the profiles, because an open port open does not necessarily mean the endpoint is functioning and accepting connections.

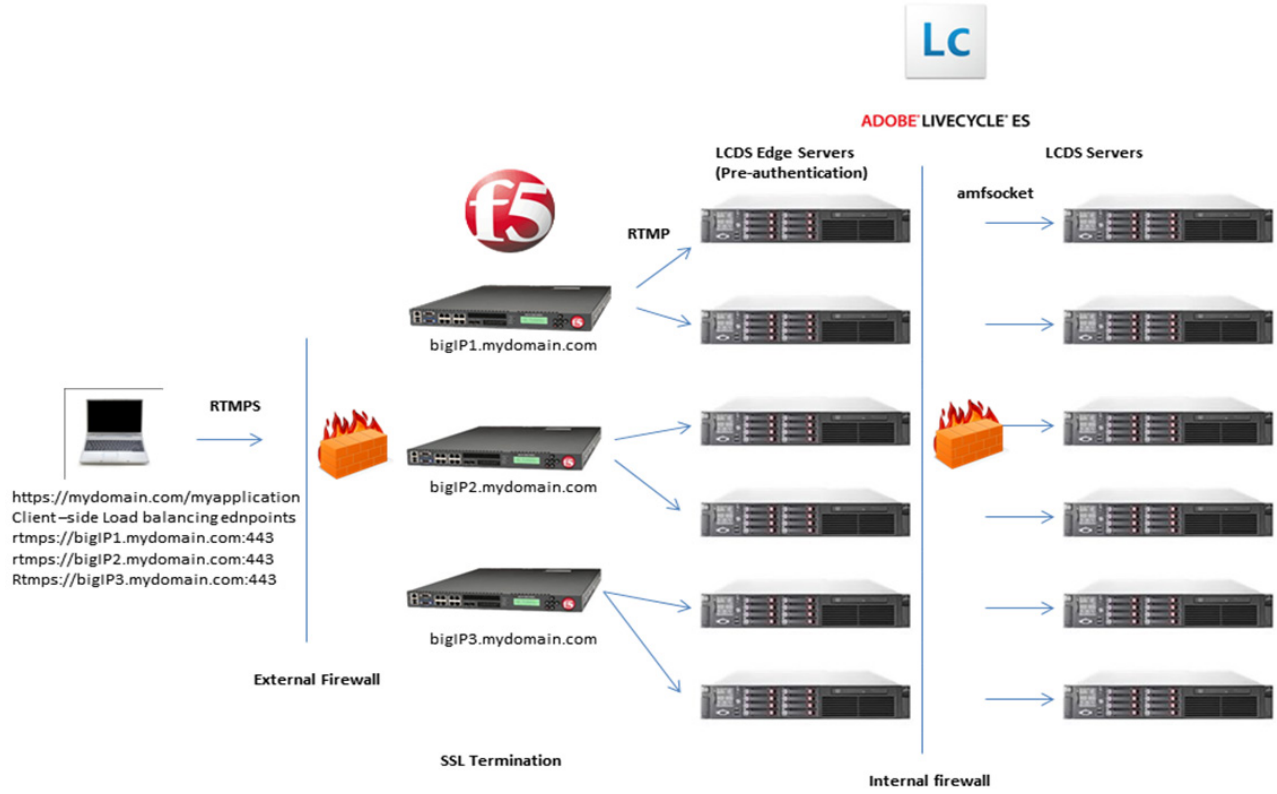


Deployment tier: A. Client; B. Edge tier; C. Server tier

Configuration for SSL termination

The following diagram shows client-side load balancing and SSL termination. A client picks a channel randomly in the client load-balancing channels. These channels connect to the F5 BIG-IP LTM for SSL termination. The F5 BIG-IP LTM also acts as a load balancer to two different LiveCycle Data Services

edge servers. The edge server connects to a Data Services server through an AMF connection for every RTMPS connection.



Client-side load balancing and F5 BIG-IP SSL termination

Load testing tool considerations

For load-balancing considerations, the F5 BIG-IP LTM should not become a bottleneck for real-time systems. Planning for load balancing should test your hardware throughput. You can measure the throughput with the load-testing tool, client, and message generator included with LiveCycle Data Services. The load testing tool can also be used for capacity planning.

When the load testing tool is run from a large number of clients, configure the load balancer to not deny multiple connections from same IP. To prevent DoS attacks, load balancers typically block an offending IP.

Channel definitions

Channel definitions are defined in the services-config.xml configuration file. The LiveCycle Data Services server instantiates the channels in this configuration file if they are not marked as remote="true". Client applications are also compiled with services-config.xml to have connectivity information. It is not necessary to have the same configuration file for the LiveCycle Data Services server and application compilation.

Two tokens can be used in the channel definition: {server.name} and {server.port}. When these two tokens appear in the channel definition, clients use the loaded application's URL domain and port to construct the endpoint URL.

Standard channel

Clients use port 1935 and connect to the server from which the application was loaded. On the server side, this endpoint binds to all NICs using port 1935.

```
<channel-definition class="mx.messaging.channels.RTMPChannel"
id="my-rtmp">
<endpoint class="flex.messaging.endpoints.RTMPEndpoint"
url="rtmp://{server.name}:1935"/>
</channel-definition>
```

Channels using bind-port

Clients connect to the server using the endpoint URL, but the endpoint actually listens on the port number specified as the value of the bind-port property. The bind-port configuration is useful when the server and client use the same services-configuration.xml file. Clients connect to a load balancer at port 1935 when the actual LiveCycle Data Services channel port is 2215.

```
<channel-definition class="mx.messaging.channels.RTMPChannel"
id="my-bigIP-rtmp" remote="true">
<endpoint class="flex.messaging.endpoints.RTMPEndpoint" url="
rtmp://bigIP.adobe.com:1935"/>
<properties>
<bind-port>2215</bind-port>
</properties>
</channel-definition>
```

Channels using bind-port with SSL termination

Clients connect to the F5 BIG-IP LTM system through an SSL channel and have SSL termination. The channel definition class is mx.messaging.channels.SecureRTMPChannel. The endpoint class is flex.messaging.endpoints.RTMPEndpoint.

```
<channel-definition class="mx.messaging.channels.SecureRTMPChannel"
id="my-biglP-rtmps">
<endpoint class="flex.messaging.endpoints.RTMPEndpoint" url="
rtmps://biglP.adobe.com:443"/>
<properties>
<bind-port>2215</bind-port>
</properties>
</channel-definition>
```

Using separate server and client services-config.xml files

Server side

```
<channel-definition class="mx.messaging.channels.RTMPChannel"
id="my-biglP-rtmps">
<endpoint class="flex.messaging.endpoints.RTMPEndpoint" url="
rtmps://biglP.adobe.com: 2215"/>
</channel-definition>
```

Client side

```
<channel-definition class="mx.messaging.channels.SecureRTMPChannel"
id="my-bigIP-rtmps">
<endpoint class="flex.messaging.endpoints.SecureRTMPEndpoint " url="
rtmps://bigIP.adobe.com: 443"/>
</channel-definition>
```

Edge server channel

The LiveCycle Data Services edge server communicates with the Data Services server over AMF socket connections.

LiveCycle Data Services server

```
<channel-definition class="mx.messaging.channels.RTMPChannel"
id="my-edge-rtmp" remote="true">
<endpoint class="flex.messagingendpoints.RTMPEndpoint" url="
rtmp://edge.adobe.com: 2215"/>
</channel-definition>
```

Edge server

```
<channel-definition class="mx.messaging.channels.RTMPChannel"
id="my-edge-rtmp">
<endpoint class="flex.messagingendpoints.RTMPEndpoint " url="
rtmp://edge.adobe.com: 2215"/>
</channel-definition>
```

Edge server pre-authentication

Set the require-authentication property to true. Only successfully authenticated connections are routed to the LiveCycle Data Services server.

```
<service class="flex.messaging.services.GatewayService"
id="perf-edge-auto-GatewayService">
<properties>
<gateway-endpoint>
<require-for-startup>true</require-for-startup>
<require-authentication>true</require-authentication>
<urls>
<url>amfsocket://lcds.adobe.com:4321</url>
```

```
</urls>
</gateway-endpoint>
</properties>
</service>
```

Edge server pre-authorization

Apply a security constraint to the gateway service. Only the users in the required role are allowed to connect to the LiveCycle Data Services server.

```
<service class="flex.messaging.services.GatewayService"
id="perf-edge-auto-GatewayService">
<default-security-constraint ref="traders-and-admins"/>
<properties>
<gateway-endpoint>
<require-for-startup>true</require-for-startup>
<urls>
<url>amfsocket://lcds.adobe.com:4321</url>
</urls>
</gateway-endpoint>
</properties>
</service>
```

Client load-balancing channel

You can use client load balancing to distribute client connections across available servers in the absence of a load balancer. Client applications compiled against an endpoint configuration with client load balancing use this set of URLs for connectivity rather than the URL specified for the endpoint.

The endpoint URL value is not compiled into the SWF file. Before the client initially connects, it shuffles this full set of URLS and assigns one at random as the primary URL for its channel. It assigns the remainder to the failover URIs property on its channel. If you use SSL termination on the F5 BIG-IP LTM system, change the channel definition class to SecureRTMPChannel. You also have to consider Flash Player security. Without the crossdomain.xml file, clients cannot connect to any server other than the location of the loaded application.

Client-side services-config.xml file

```
<channel-definition id="my-http" class="mx.messaging.channels.RTMPChannel
" >
<endpoint url=" rtmp://lcds1.adobe.com:2215" class="
flex.messaging.endpoints.RTMPEndpoint"/>
<properties>
<client-load-balancing>
<url>rtmp://lcds1.adobe.com:2215</url>
<url> rtmp://lcds2.adobe.com:2215</url>
<url> rtmp://lcds3.adobe.com:2215</url>
</client-load-balancing>
</properties>
</channel-definition>
```

Gateway endpoint tuning on the Live Cycle Data Services server

If the gateway endpoint in the LiveCycle Data Services server configuration does not have a server-ref value, the endpoint creates a server with the default settings. For high message volume, define a server for the gateway endpoint and increase the buffer size and number of worker threads.

Changing these settings can greatly improve performance. The message latency can be brought down from tens of milliseconds (ms) to several milliseconds. In testing, with a send rate of 60,000 messages per second and a 1 kilobyte payload size, the message latency was 72 ms when using the default server settings. By increasing the buffer sizes, the message latency was brought down to 5 ms.

LiveCycle Data Services server services-config.xml file for the gateway endpoint

To prevent reconnections, the value of `session-timeout-minutes` parameter can be increased.

```
<server class="flex.messaging.socketserver.SocketServer"
id="perf-nio-edge-server">
<properties>
<connection-read-buffer-size>8192</connection-read-buffer-size>
<connection-write-buffer-size>65536</connection-write-buffer-size>
<socket-receive-buffer-size>8192</socket-receive-buffer-size>
<socket-send-buffer-size>65536</socket-send-buffer-size>
<connection-buffer-type>heap</connection-buffer-type>
<socket-tcp-no-delay-enabled>true</socket-tcp-no-delay-enabled>
<worker-thread-priority>5</worker-thread-priority>
<reactor-count>8</reactor-count>
<http>
<session-timeout-minutes>l</session-timeout-minutes>
</http>
</properties>
</server>
<channel-definition id="gateway-endpoint" server-only="true" >
<endpoint class="flex.messaging.endpoints.GatewayEndpoint"
url="amfsocket://localhost:9807"/>
<server ref="perf-nio-edge-server"/>
</channel-definition>
```

BIG-IP LTM system configuration for use with RTMP endpoints

Configuring the F5 BIG-IP LTM system to direct requests to an RTMP endpoint involves the following steps:

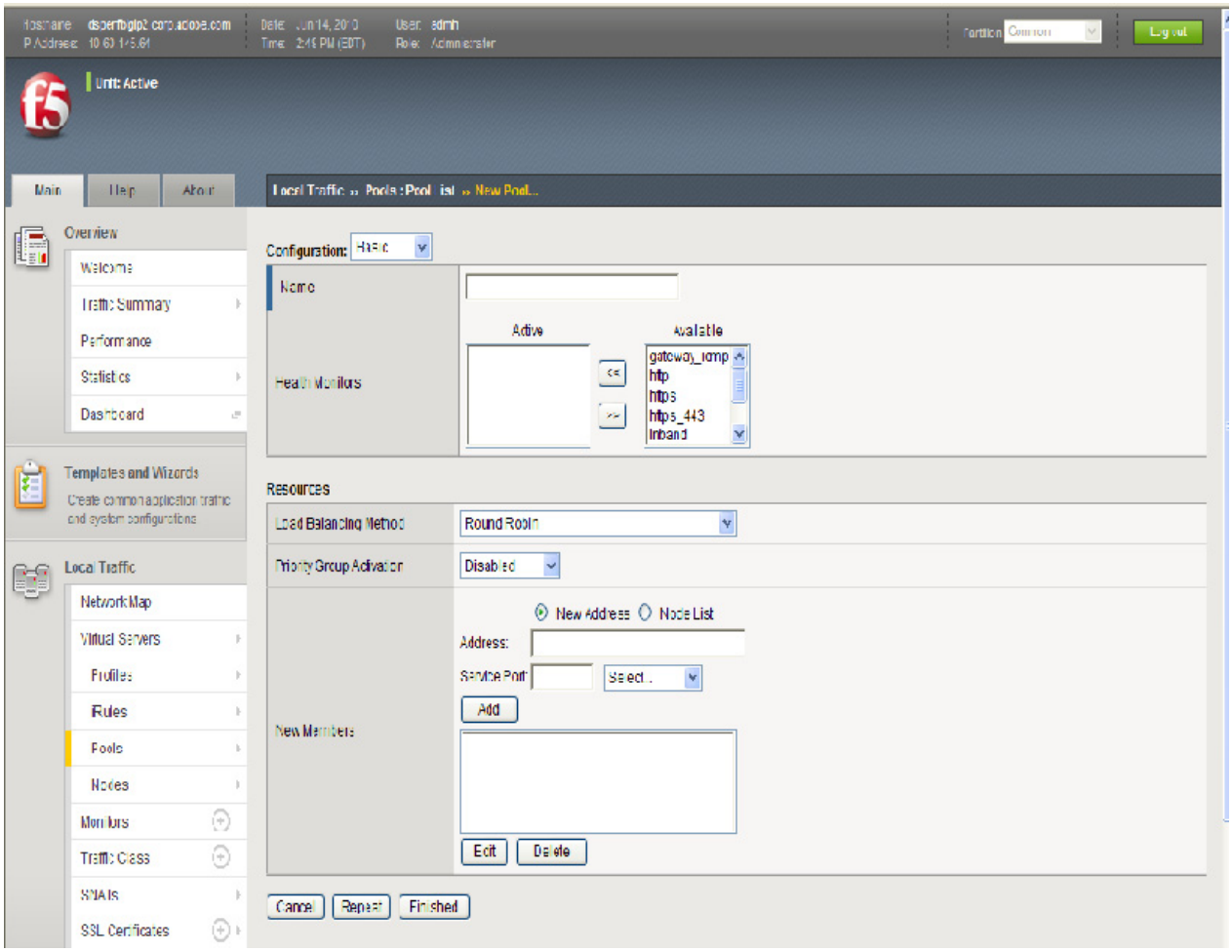
1. (Optional) Create a health monitor.
2. Create a LiveCycle Data Services RTMP pool.
3. Create profiles.
4. Create a virtual server.

Create the TCP health monitor

1. On the Main tab, expand Local Traffic, and then click Monitors.
2. Click the Create button. The New Monitor screen opens.
3. In the Name box, type a name for the monitor (for example, qa-perf-edge-rtmp).
4. From the Type list, select tcp.
5. In the Configuration section, in the Interval and Timeout boxes, type an interval and timeout.
6. Click Finished.

Create the LiveCycle Data Services server pool

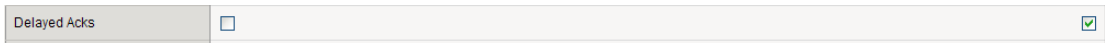
1. On the Main tab, expand Local Traffic.
2. Go to Pools and select Pool List.
3. Click the Create button.
4. Enter the name (for example, lcds-edge-pool).
5. (Optional) Select the health monitor.
6. Select the load balancing method. For information about load balancing methods, see this article. As RTMP is an open connection, Round Robin cannot evenly distribute its load. Select Least Connections as the load balancing method.
7. Add the endpoint port address and service port for all Data Services servers.
8. Click Finished.



Create the profile for low message latency

1. On the Main tab, expand Local Traffic.
2. Click Profiles and select TCP protocol.
3. Click Create.
4. Enter the name (for example, lcds-edge-profile).
5. For the parent profile, select tcp-wan-optimized.
6. Select the following values for these settings:
    - Delay Acks: disabled.
    - Selective Acks: disabled.
    - Slow Start: disabled.
    - Bandwidth Delay: disabled.
    - Nagle's Algorithm: disabled.

7. Click Finished.

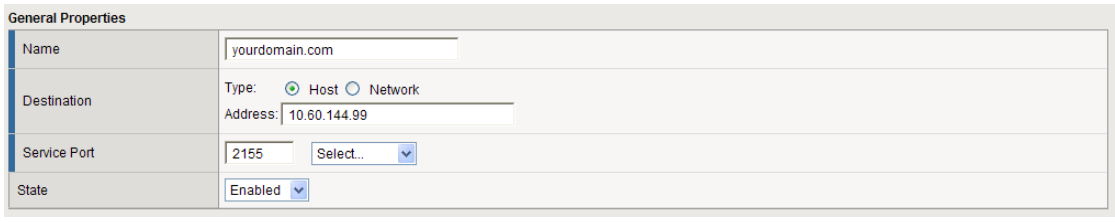


Create the client SSL profile

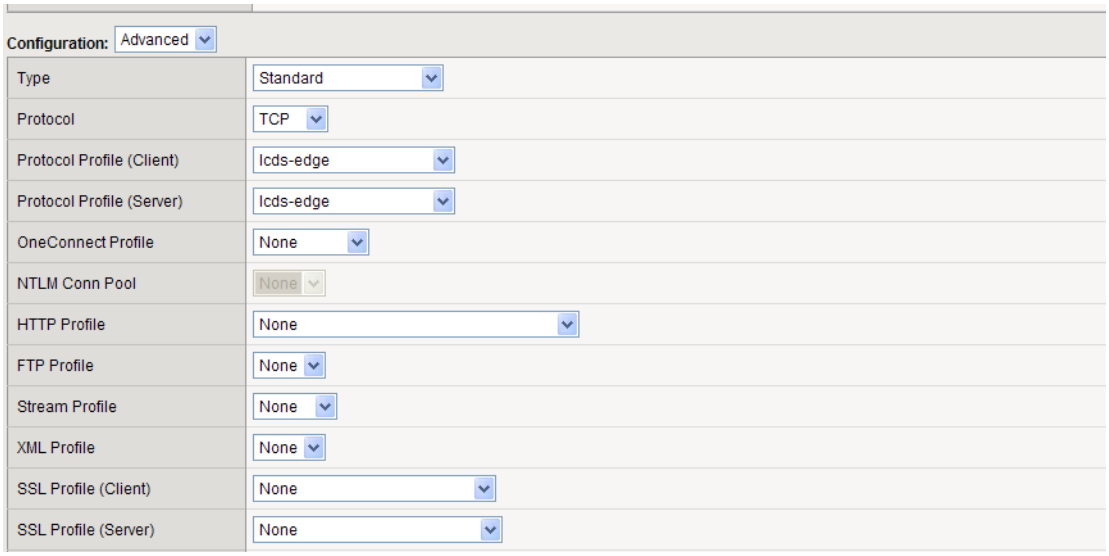
1. On the Main tab, expand Local Traffic, and then click Profiles.
2. Choose SSL > Client.
3. Click the Create button.
4. Enter the name for this profile (for example, lcds-ssl-profile).
5. In the Configuration section, select Custom.
6. Select your certification. (See the BIG-IP documentation for creating and importing keys and certifications.)
7. Select your key.
8. Click Finished.

Creating a virtual server

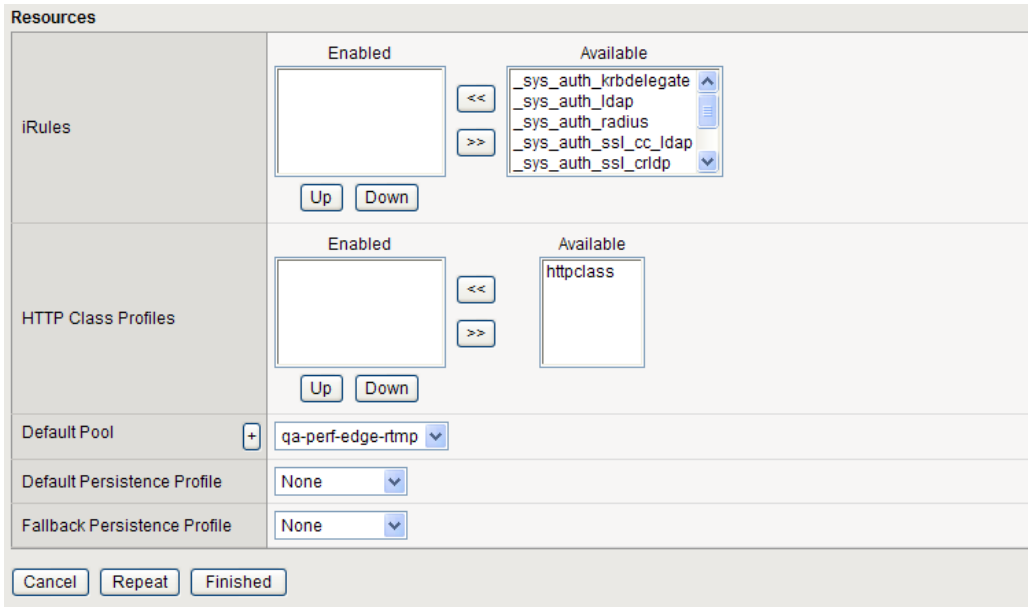
1. On the Main tab, expand Local Traffic, and then click Virtual Servers.
2. Click the Create button.
3. Enter the server name (for example, lcds-server).
4. Enter the address for the virtual server and the port (Data Services channel endpoint).



5. From the Configuration drop-down menu, select Advanced.
6. For the client and server protocol profiles, select the one that was created (lcds-edge-profile).
7. For OneConnect Profile, choose None.
8. For SSL Profile (Client), enter your SSL profile if you want SSL termination (lcds-ssl-profile).



9. For the default pool, use the created TCP pool (lcds-edge-pool).
10. Click Finished.



Test results with and without BIG -IP LTM

The results below demonstrate that the additional hop added with an F5 BIG-IP LTM is negligible when properly configured. Test results using the Data Services load-testing tool are presented below.

Results without the BIG-IP LTM

[INFO] [RtmpTest] Virtual Consumer avg receive rate: 119.97 msg/s

[INFO] [RtmpTest] Virtual Consumer min receive rate: 119.87 msg/s (25201 msgs in 210.23s)

[INFO] [RtmpTest] Virtual Consumer max receive rate: 120.0 msg/s (25541 msgs in 212.85s)

[INFO] [RtmpTest] Virtual Consumer avg latency: 3.79 ms

[INFO] [RtmpTest] Virtual Consumer min latency: 0 ms

[INFO] [RtmpTest] Virtual Consumer max latency: 53 ms

[INFO] [RtmpTest] Virtual consumer std latency: 4.91 ms

Results with the BIG-IP LTM

[INFO] [RtmpTest] Virtual Consumer avg receive rate: 119.77 msg/s

[INFO] [RtmpTest] Virtual Consumer min receive rate: 119.69 msg/s (25323 msgs in 211.575)

[INFO] [RtmpTest] Virtual Consumer max receive rate: 119.8 msg/s (25181 msgs in 210.195)

[INFO] [RtmpTest] Virtual Consumer avg latency: 4.97 ms

[INFO] [RtmpTest] Virtual Consumer min latency: 2 ms

[INFO] [RtmpTest] Virtual Consumer max latency: 53 ms

[INFO] [RtmpTest] Virtual consumer std latency: 3.71 ms

Useful links

Using Adobe® LiveCycle® Data Services ES3

Deploying the BIG-IP LTM System with Adobe Connect web conferencing software

BIG-IP Systems: Getting Started Guide

About Adobe LiveCycle Data Services

The Adobe® LiveCycle® Data Services module provides the most powerful set of real-time data management and messaging capabilities available in the rich Internet application (RIA) space today. Leverage this scalable and optimized framework to abstract the complexity and cost of building easy-to-use, personalized, and interactive applications that take advantage of rich, real-time data. Take advantage of powerful, model-driven development tools as well as additional features that streamline development, ease data and client integration, and facilitate easier deployment of RIAs. LiveCycle Data Services can also be extended beyond firewalls more securely with NIO-enabled endpoints that further optimize tiered server resources as well as provide authentication for access to internal feeds.

About BIG- IP systems

The BIG-IPT® system is a set of application delivery products that work together to ensure high availability, improved performance, application security, and access control. The primary module in the product family, the Local Traffic Manager, directs different types of protocol and application traffic to an appropriate destination server. Other modules available on the BIG-IP system provide critical functions such as WAN Optimization Module, which optimizes connections across a wide-area network, the WebAccelerator system, which accelerates HTTP connections, Application Security Manager, which applies security policies to network traffic, and Global Traffic Manager, which maintains responsive user access regardless of network conditions.

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

November 2012